HIPAA FISCAL AGENT PROVIDER ANNUAL TRAINING

As a Fiscal Agent Provider of CLTS Waiver covered services
you are expected to protect your Client's Personal Health Information (PHI).
You are accountable
to the Client and the State and Federal Government
for protection of the Client's PHI.

Why is Privacy and Security Training Important?

- It outlines ways to prevent accidental and intentional misuse of PHI
- To make PHI secure
- Its not just about HIPAA – it is about doing the right thing!
- Providers are required to do it

Parent/Guardian Responsibility

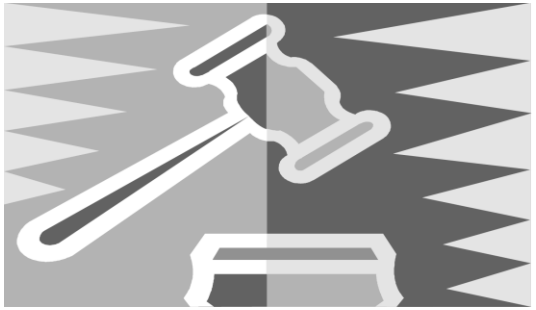
- Acting on behalf of the Client
- Setting up policies and training for use, storage and disposal of the Client's PHI
- Reviewing training with the Fiscal Agent Provider
- Holding the Fiscal Agent Provider accountable for protection of PHI
- Waukesha County is not the employer of the Fiscal Agent Provider and assumes no authority over, or responsibility for, the actions of the Employer or the Fiscal Agent Provider

Why is Privacy and Security Training Important?

- We should treat personal electronic data with the same care and respect as weapons-grade plutonium -- it is dangerous, long-lasting and once it has leaked there's no getting it back.

  -- Corey Doctorow

What is HIPAA?



- **HIPAA** stands for

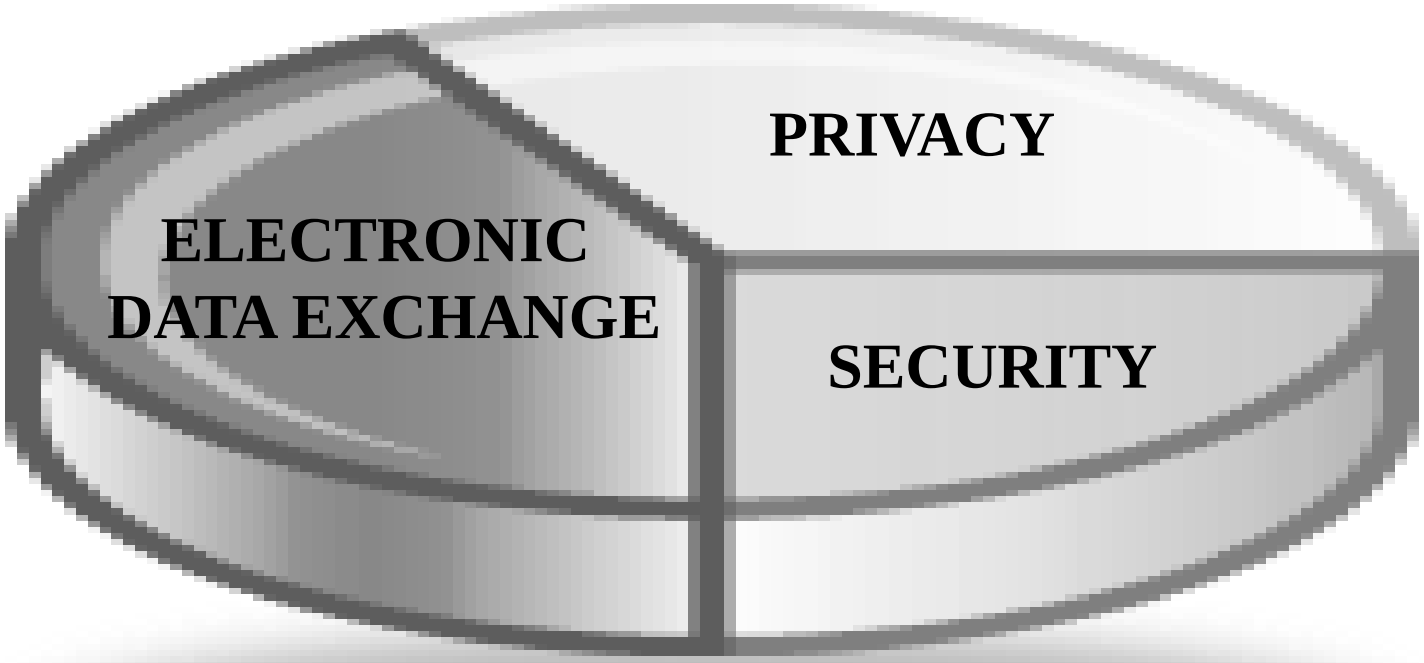
  Health **I**nsurance **P**ortability and **A**ccountability **A**ct
- Originally it focused on ensuring the portability of health insurance for individuals and improving fraud and abuse protections – passed in 1996
- Provides the framework for the establishment of:
  - A nationwide protection of the confidentiality of health information
  - Security standards and
  - Standards and requirements for the electronic transmission of health information

What is HIPAA?

- A federal act (law) that sets provisions for use of client/patient information by health care agencies
  - Federal Regulation 45 CFR Parts 160,162 and 164
- Gives individuals more control and access to their medical information
- A law that protects individually identifiable medical information from threats of loss or disclosure
- Simplifies the administration of health insurance claims and lower costs
- Mandates the standardization of electronic data exchange

HIPAA has Three Parts:

Each part has separate regulations to comply with HIPAA mandates accountability



What is Protected Health Information (PHI)?

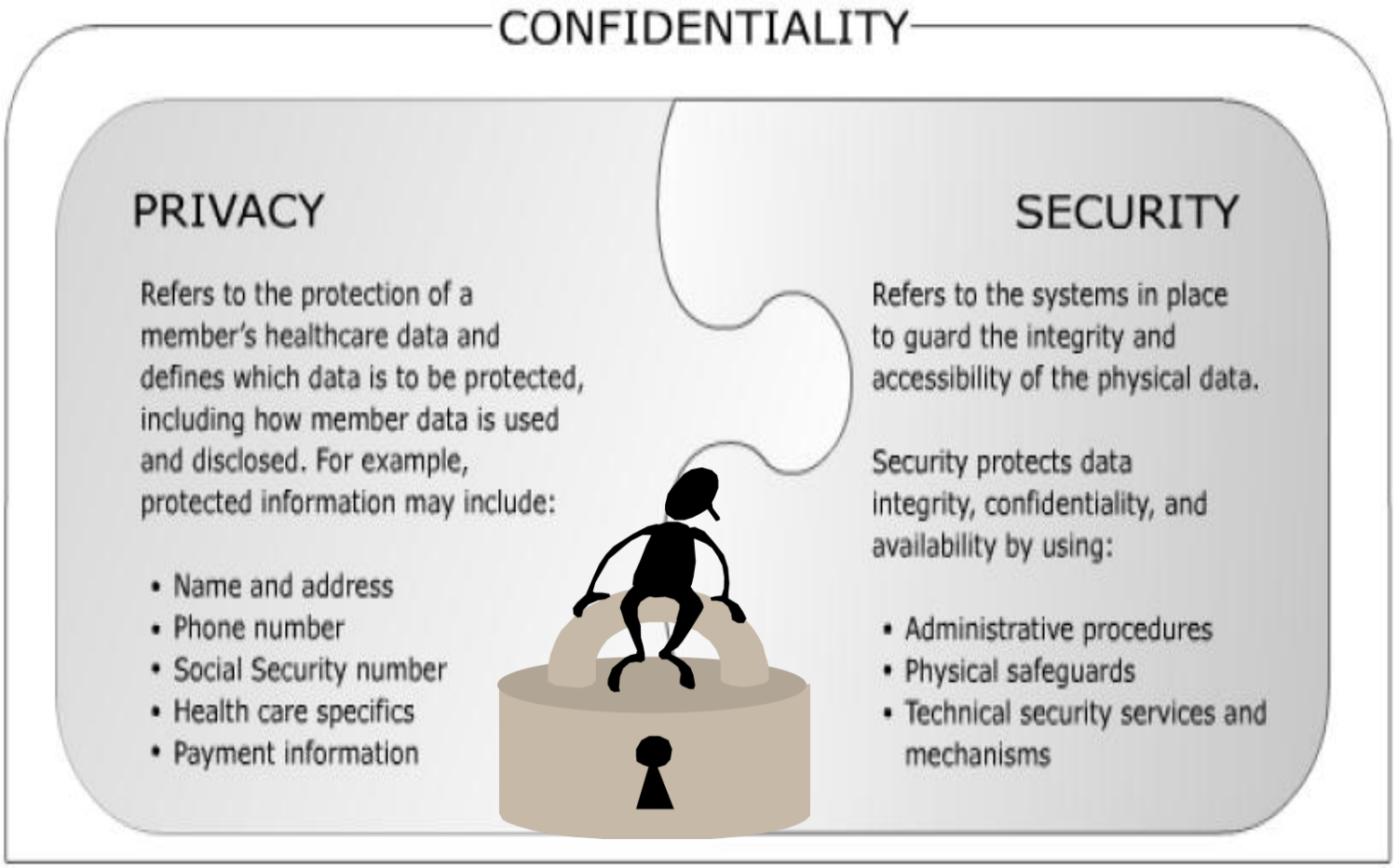
- PHI is individually identifiable health information relating to information:
  - That reveals the physical or mental state of a person's health
  - About the payment for the health care services of an individual
  - That identifies with reasonable accuracy and speed the identity of a client
- Information can be in the form of:
  - Written
  - Oral
  - Email
  - Other computer generated health information that reveals the identity of the person

Who or What Protects PHI?

1. The Federal Government through the laws of HIPAA

2. You, the Fiscal Agent Provider, by following policies and procedures

To Maintain Confidentiality- We Need Both Privacy and Security



What is the HIPAA Privacy Rule?

- The Privacy Regulations went into effect

  April 14, 2003

- Privacy refers to the protection of an individual's health care data/information
- Defines how client information is used and disclosed

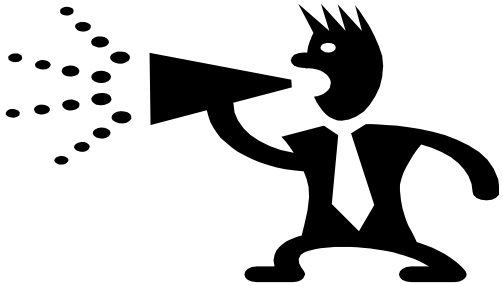
Why is the Privacy Rule Important?

- Gives individuals rights to control the use and disclosure of their PHI
- Puts boundaries on the use of health care information
- Sets procedures for maintaining past, present and future patient records
- Sets procedures for the sharing and maintaining of written, electronic and verbal client/patient information

INDIVIDUALLY IDENTIFIABLE INFORMATION-PHI that Needs to be Protected-Both Written and Verbal

1. Name
2. Geographic subdivisions smaller than a State
   - Street Address
   - City
   - County
   - Precinct
   - Zip Code/Equivalent Geocodes
3. Dates, except year
   - Birth date
   - Admission date
   - Discharge date
   - Date of death
4. Telephone numbers
5. Fax number
6. E-Mail Address
7. Social security numbers
8. Medical record numbers
9. Health plan beneficiary numbers
10. Account numbers
11. Certificate/license numbers
12. Vehicle identifiers and serial numbers, including license plate numbers
13. Device identifiers and serial numbers
14. Web universal resource locations (URLs)
15. Internet Protocol (IP) address numbers
16. Biometric identifiers, including finger and voice prints
17. Full face photographic images and any comparable images
18. Any other unique identifying number, characteristic, or code

What are Examples of Verbal PHI That Must be Protected?



- Appointment reminders left on answering machines. The message should be brief – ID area, date and time of appointment
- Talking about clients in areas that can be overhead by others, especially the public
- Telephone calls where the public can overhear conversations where PHI is discussed

How Do You Know What PHI You Can Access?

- Ask yourself "Do I need this information to do my job?"
- This is the first check. If you don't need it to do your job, you shouldn't be using it

What is Misuse of Protected Health Information?

U n a u t h o r i z e d:

- Access to…….
- Using…..
- Taking……..
- Possession of……..
- Release of …….
- Edit of ……..
- Destruction of……

PHI Without Authorization

What is the HIPAA Security Rule?

- The security policies requires that we:
  - Know our policies, standards and procedures
  - Apply physical safeguards
  - Apply technical safeguards
  - Outline ways we can prevent accidental and intentional misuse of protected information

How to Apply the Security Rule?

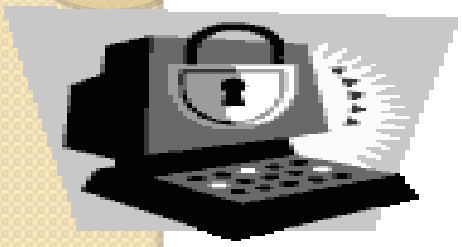
Administrative Safeguards –

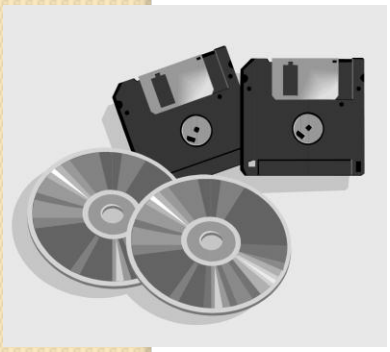
Policies and procedures are REQUIRED and they define what needs to be done to maintain security

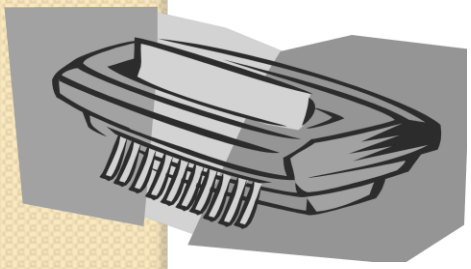
Sample Policies include:

- The use of the internet
- Use of email – what can and cannot be emailed
- How to fax properly
- Use of voicemail
- How systems containing PHI will be secured

How to Apply the Security Rule?







Technical Safeguards –

Many technical devices are needed to maintain security

Examples include:

- Different levels of computer passwords
- Screen savers
- Data backups
- Safe disposal of videos, emails, computer files
- Encryption

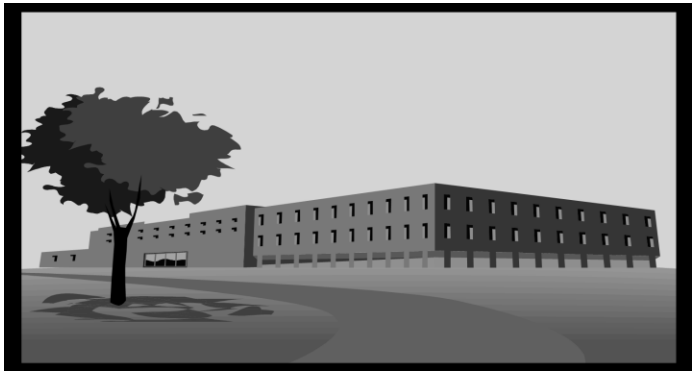
How to Apply the Security Rule?

Physical Safeguards –

Many physical barriers and devices are needed to maintain security

Examples include:

- Locks on doors
- Identifying visitors
- Locking containers to protect the client's PHI



How to Apply the Security Rule?

Personnel Security –

Policies and procedures that manage the assignment of access authority to employees and other workforce members

- Procedures address employee transfers, role changes and terminations-
- As a person's role changes, so does their access to certain systems
- Effective security and privacy training must be conducted.

Penalties for Breach of Patient Confidentiality - WI

- WI Stat 51.30
  - Knowing and willful disclosure
    - Up to $25, 000 plus actual damages and attorney fees
  - Negligent disclosure
    - $1,000 plus actual damages and attorney fees per violation
  - Requests/obtains information under false pretenses
    - $25,000 or imprisonment for up to 9 months or both
  - Discloses information knowing that the disclosure is unlawful and not necessary to protect another from harm
    - $25,000 or imprisonment for up to 9 months or both

Penalties for Breach of Patient Confidentiality - WI

- Falsification, obstruction, investigation, intentional destruction or damages records
  - $25,000 or imprisonment for up to 9 months or both

- Intentional disclosure, knowing the information is confidential and discloses for monetary gain
  - $100,000 or imprisoned 3.5 years or both

- Provider may be suspended or discharged without pay

Penalties for Breach of Patient Confidentiality - HIPAA Sanctions

- Civil Penalties:

Violation	Penalty	Maximum Penalty
Individual did not know they violated HIPAA	$100 per violation, with an annual max. of $25,000 for repeat violations	$50,000 per violation, with an annual max. of $1.5 million
Due to reasonable cause/not willful neglect	$1,000 per violation, with an annual max. of $100,000 for repeat violations	$50,000 per violation, with an annual max. of $1.5 million

Penalties for Breach of Patient Confidentiality - HIPAA Sanctions

- Civil Penalties Continued:

Violation	Penalty	Maximum Penalty
Due to willful neglect but violation is corrected within required time period	$10,000 per violation, with an annual max. of $250,000 for repeat violations	$50,000 per violation, with an annual max. of $1.5 million
Due to willful neglect but not corrected	$50,000 per violation, with an annual max. of $1.5 million	$50,000 per violation, with an annual max. of $1.5 million

Penalties for Breach of Patient Confidentiality - HIPAA Sanctions

- Criminal Penalties – improperly obtaining or disclosure of PHI or improperly use unique health identifiers are subject to the following penalties:

Penalty	Fine	Prison time
Knowingly	$50,000	Up to 1 year
Under false pretenses	$100,000	Not more than 5 yrs
For profit, gain or harm	$250,000	Not more than 10 yrs

Access Violation – Access of PHI by a Coworker

- Parents of clients or providers ask for or share information regarding other clients or former clients
- Is this against HIPAA policies?

Access Violation

- **Yes.**
- It is inappropriate to ask for or share any information with parents or providers of clients if it is not part of their regular assigned job responsibilities

ROI: Talking with Friends About Work

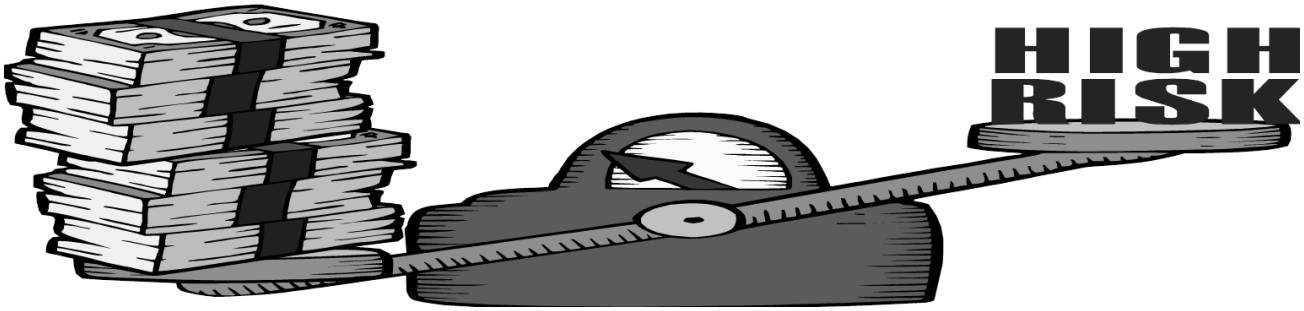
- You had a negative encounter with a patient/client or overhead a negative encounter and really need to vent to a friend or spouse after work. What can you discuss?
  - Working in health care isn't easy and patient confidentiality MUST be maintained at all times –
    - At work
    - During non-work hours
    - Even after your employment with the child and/or family ends
  - Here are some helpful tips……

ROI: Talking with Friends About Work

- Do not share with family, friends, or anyone else a patient's name, or any other information that may identify him/her, for instance:
  - It would ***not*** be a good idea to tell anyone that a patient came in to be seen after an incident with the police
    - **Why**? Your friend may hear about the police incident on the news and know the person involved
- Do not inform anyone that you know a famous person, or their family member, was seen at our organization
- **<u>Do Not</u> swear your family, friends or anyone else to secrecy that they will not tell your story to anyone else**

1. Be Knowledgeable – Understand the HIPAA Policies

- Read and understand HIPAA policies as <u>you</u> will be held directly accountable
- The client and his/her family is placing trust in you to follow the policies
- Choosing not to follow these rules
  - **Could put you at risk**



2. *Think Before You Share/Disclose Client Information in Public Areas*

- Discussions should occur in private areas
- If you must have the discussion in a public area, keep your voice low
- Remember- you can be overheard anywhere

3. Think Before You Share Information- Releasing Information

- Share client information only with authorized individuals
- In most cases, a written authorization is required for client information to be released

4. Protect Access to Information

If you **DO NOT** need
certain information to do your job…..

- **DON'T ASK**
- **DON'T READ IT**
- **DON'T BE NOSEY**

5. Keep Information Out of Site From the Public

- Close records/charts/files when not in use
- Cover clipboards

- Never leave paper with PHI unattended

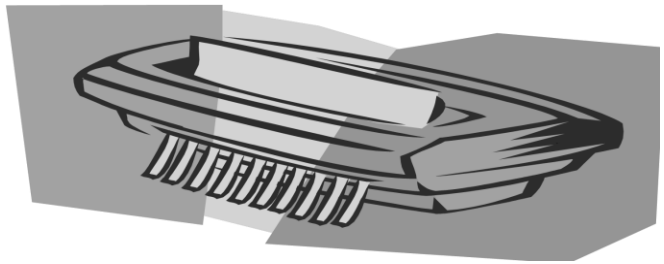
- <u>If you need to take information with client names (i.e. client pick up names, work calendar with client names) home or in your vehicle, you are responsible for the safe keeping of such items</u>

6. Be Cautious with Technology –EMAIL

- Email - never e-mail protected Patient/Client information unless using secure email
- Do not put PHI in the subject line of an email
- Contact the Parent/Guardian for direction

7. Properly Destroy Client Information

- Any paper with confidential patient information on it that is to be destroyed shall be given to the client's parent/guardian for shredding



How and Whom Do You Report a Concern To ?

- It is your duty to report any concerns you have about privacy and security
- Tell the Parent/Guardian right away
- Tell the Client's service coordinator right away

What it Means to be a Fiscal Agent Provider

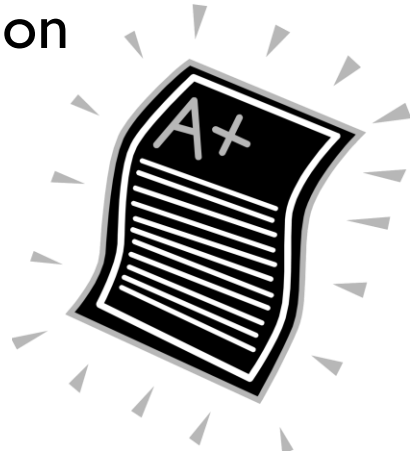
- The Fiscal Agent Provider is an employee of the Client with Parent/Guardian acting as employer on the Client's behalf

- The Fiscal Agent Provider is responsible to the employer for performance of duties and maintenance of standards

- Waukesha County is <u>not</u> the employer of the Fiscal Agent Provider and assumes no authority over, or responsibility for, the actions of the Employer or the Fiscal Agent Provider

To receive credit for this training:
Complete the following forms and
Send to the client's service coordinator:

- The **Training Acknowledgment Form**
  - Read it
  - Complete test and record test answers on this form
  - Sign it



- The **Confidentiality/Non-Disclosure Statement**
  - Read it
  - Sign it